reports, information and assistance as may be necessary, and

(3) Serve as the principal advisor to the Assistant Secretary (Management) with respect to Treasury physical and information security programs.

§ 2.39 Bureau administration.

Each Treasury bureau and the Departmental Offices shall designate, in writing to the Departmental Director of Security, an officer or official to direct, coordinate and administer its physical security and information security programs which shall include active oversight to ensure effective implementation of the Order, the Directive, this regulation. Bureaus and the Departmental Offices shall revise their existing implementing regulation on national security information to ensure conformance with this regulation. Time frames for bureau and Departmental Offices implementation shall be established by the Departmental Director of Security.

§ 2.40 Emergency planning [4.1(b)].

Each Treasury bureau and the Departmental Offices shall develop plans for the protection, removal, or destruction of classified information in case of fire, natural disaster, civil disturbance, or possible enemy action. These plans shall include the disposition of classified information located in foreign countries.

§ 2.41 Emergency authority [4.1(b)].

The Secretary of the Treasury may prescribe by regulation special provisions for the dissemination, transmittal, destruction, and safeguarding of national security information during combat or other emergency situations which pose an imminent threat to national security information.

§ 2.42 Security education [5.3(a)].

Each Treasury bureau that creates, processes or handles national secutity information, including the Departmental Offices, is required to establish a security education program. The program shall be sufficient to familiarize all necessary personnel with the provisions of the Order, the Directive, this regulation and any other implementing directives and regulations to impress upon them their individual security responsibilities. The program shall also provide for initial, refresher, and termination briefings.

(a) *Briefing of Employees.* All new employees concerned with classified information shall be afforded a security briefing regarding the Order, the Directive and this regulation and sign a security agreement as required in § 2.22(c). Employees concerned with sensitive compartmented information shall be required to read and also sign a security agreement. Copies of applicable laws and pertinent security regulations setting forth the procedures for the protection and disclosure of classified information shall be available for all new employees afforded a security briefing. All employees given a security briefing shall be required to sign a TD F 71–01.16 (Physical Security Orientation Acknowledgment) which shall be maintained on file as determined by respective office or bureau security officials.

(b) [Reserved]

Subpart F—General Provisions

§ 2.43 Definitions [6.1].

(a) *Authorized Person.* Those individuals who have a ''need-to-know'' the classified information involved and have been cleared for the receipt of such information. Responsibility for determining whether individuals' duties require that they possess, or have access to, any classified information and whether they are authorized to receive it rests on the individual who has possession, knowledge, or control of the information involved, and not on the prospective recipients.

(b) *Compromise.* The loss of security enabling unauthorized access to classified information. Affected information or material is not automatically declassified.

(c) *Confidential Source.* Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

(d) *Declassification.* The determination that particular classified information no longer requires protection against unauthorized disclosure in the interest of national security. Such determination shall be by specific action or occur automatically after the lapse of a requisite period of time or the occurrence of a specified event. If such determination is by specific action, the information or material shall be so marked with the new designation.

(e) *Derivative Classification.* A determination that information is, in substance, the same as informaiton that is currently classified and a designation of the level of classification.

(f) *Designated Countries of Concern.* For purposes of National Security Decision Directive 197 reporting: Afghanistan, Albania, Angola, Bulgaria, Cambodia (Kampuchea), the People's Republic of China (Communist China), Cuba, Czechoslovakia, Ethiopia, East Germany (German Democratic Republic including the Soviet sector of Berlin), Hungary, Iran, Iraq, Laos, Libya, Mongolian People's Republic (Outer Mongolia), Nicaragua, North Korea, Palestine Liberation Organization, Poland, Romania, South Africa, South Yemen, Syria, Taiwan, Union of Soviet Socialist Republics (Russia), Vietnam and Yugoslavia.

(g) *Document.* Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed material; data processing cards and tapes; maps, charts; painting; drawings; engravings; sketches; working notes and papers; reproductions of such things by any means or process; and sound, voice, or electronic recordings in any form.

(h) *Foreign Government Information.* (1) Information provided by a foreign government or governments, an international organization of governments, or any elements thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) Information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

(i) *Information.* Any data or material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(j) *Information Security.* The administrative policies and procedures for identifying, controlling, and safeguarding from unauthorized disclosure, information the protection of which is authorized by Executive Order or statute.

(k) *Intelligence Activity.* An activity that an agency within the Intelligence Community is authorized to conduct pursuant to Executive Order 12333.

(l) *Intelligence Sources and Methods.* A person, organization, or technical means or method which provides foreign intelligence or foreign counterintelligence to the United States and which, if its identity or capability is disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness in providing foreign intelligence or foreign counterintelligence to the United States. An intelligence source also means a person or organization which provides foreign intelligence or foreign counterintelligence to the United States only on the condition that its identity remains undisclosed. Intelligence methods are that which, if disclosed, reasonably could lead to the disclosure of an intelligence source or operation.

(m) *Limited Official Use.* The legend authorized for ''Officially Limited Information'' which provides that it be handled, safeguarded and stored in a manner equivalent to national security information classified Confidential.

(n) *Multiple Classified Sources.* The term used to indicate that a document is derivatively classified when it contains classified information derived from other than one source.

(o) *National Security.* The national defense or foreign relations of the United States.

(p) *National Security Information.* Information that has been determined

pursuant to the Order or any predecessor Executive Order to require protection against unauthorized disclosure and that is so designated.

(q) *Need-to-Know.* A determination made by the possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of particular work, including performance on contracts for which such access is required.

(r) *Officially Limited Information.* Information which does not meet the criterion that unauthorized disclosure would at least cause damage to the national security under the Order or a predecessor Executive Order, but which concerns important, delicate, sensitive or proprietary information which is utilized in the development of Treasury policy. This includes the enforcement of criminal and civil laws relating to Treasury operations, the making of decisions on personnel matters and the consideration of financial information provided in confidence.

(s) *Original Classification.* An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

(t) *Original Classification Authority.* The authority vested in an Executive Branch official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

(u) *Originating Agency.* The agency responsible for the initial determination that particular information is classified.

(v) *Portion.* A segment of a document for purposes of expressing a unified theme; ordinarily a paragraph.

(w) *Sensitive Compartmented Information.* Information and material concerning or derived from intelligence sources, methods, or analytical processes, that requires special controls for restricting handling within compartmented intelligence systems established by the Director of Central Intelligence and for which compartmentation is established.

(x) *Special Access Program.* Any program imposing ''need-to-know'' or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program may include, but is not limited to, special clearance, adjudication, or investigative requirements, special designations of officials authorized to determine ''need-to-know'' or special lists of persons determined to have a ''need-to-know''.

(y) *Special Activity.* An activity conducted in support of national foreign policy objectives abroad which is planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activity, but which is not intended to influence United States political processes, public opinion, policies or media and does not include diplomatic activities or the collection and production of intelligence or related support functions.

(z) *Unauthorized Disclosure.* A communication or physical transfer of classified information to an unauthorized recipient. It includes the unauthorized disclosure of classified information in a newspaper, journal, or other publication where such information is traceable due to a direct quotation or other uniquely identifiable fact.

PART 3—CLAIMS REGULATIONS AND INDEMNIFICATION OF DEPARTMENT OF TREASURY EMPLOYEES

Subpart A—Claims Under the Federal Tort Claims Act

Subpart B—Claims Under the Small Claims Act